

<<Date>> (Format: Month Day, Year)

```
<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>> <<Address1>> <<Address2>> <<City>>, <<State>> <<Zip>>
```

#### **Data Breach Notification**

#### Dear <<First Name>> <<Last Name>>.

We are writing to provide you an important communication regarding your personal and health information which may have been compromised. We take patient privacy very seriously, and it is important to us that you are made fully aware of a recent event.

We provide patient eligibility detection and billing services for the County of Los Angeles (County). As a business associate of the County, we respect the privacy of your information and we are writing to notify you of a data breach that may involve some of your personal information.

# **Brief Description of the Incident**

On March 28, 2019, a Nemadji employee fell victim to an email phishing attack. A phishing email tries to trick someone into giving up important information by appearing to come from a reliable source. Email accounts are used by employees to communicate about and perform services for the County Department of Health Services (DHS). The phishing email compromised one email account and led to the data breach we are currently notifying you of.

As a recipient of DHS services, information concerning you, which is described below, was identified in one or more of these emails and may have been compromised.

#### What Information Was Involved

The information may have included your << ClientDef1(Breach Details Variable Text)>>.

# Actions We Are Taking in Response to this Incident

Nemadji values your privacy and deeply regrets that this incident occurred. Upon discovering the breach, we immediately took steps to prevent further access and began working closely with cybersecurity vendors to ensure that the incident is properly addressed. Nemadji has initiated an administrative review, reviewed and revised processes to enhance security, and implemented additional controls designed to prevent the recurrence of such an incident. Additionally, Nemadji has also enhanced our workforce training to identify and respond to phishing emails.

In addition to notifying individuals potentially impacted by this incident, we have notified the Federal Bureau of Investigation. We will also notify the State Attorney General's Office and the U.S. Department of Health & Human Services' Office for Civil Rights as required by law.

# What You Can Do

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.



<<Date>> (Format: Month Day, Year)

```
<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>> <<Address1>> <<Address2>> <<City>>, <<State>> <<Zip>>
```

# Notificación sobre filtración de información

#### Estimado <<First Name>> <<Last Name>>,

Le escribimos para proporcionarle una comunicación importante con respecto a su información personal y de salud que puede llegar a estar comprometida. Consideramos que la privacidad de los pacientes es un asunto serio y para nosotros es importante que esté en pleno conocimiento de un acontecimiento reciente.

Ofrecemos servicios de facturación y detección de elegibilidad de pacientes para el condado de Los Ángeles (el Condado). Como socios comerciales del Condado, respetamos la privacidad de su información y le escribimos para notificarle sobre una filtración de información que podría involucrar parte de su información personal.

# Descripción breve del incidente

El 28 de marzo de 2019, un empleado de Nemadji fue víctima de un ataque de phishing por correo electrónico. Un correo electrónico de phishing es aquel que intenta engañar a alguien para que revele información importante al hacerse pasar como proveniente de una fuente confiable. Los empleados usan las cuentas de correo electrónico para comunicar y prestar servicios para el Departamento de Servicios de Salud (DHS) del Condado. El correo electrónico de phishing puso en riesgo una cuenta de correo electrónico y provocó que se filtrara la información que en esta oportunidad le estamos notificando.

Como beneficiario de los servicios del DHS, se identificó la siguiente información que le concierne a usted en uno o más de estos correos electrónicos y quizás esté comprometida.

## Qué información se vio involucrada

La información puede haber incluido su <<Cli>intDef1(Breach Details Variable Text)>>.

# Medidas que estamos tomando como respuesta ante este incidente

Nemadji valora su privacidad y lamenta profundamente que haya ocurrido este incidente. Una vez que descubrimos la filtración, de inmediato tomamos algunas medidas para evitar otro acceso indebido y comenzamos a trabajar estrechamente con proveedores de seguridad cibernética para garantizar que el incidente se aborde de forma correcta. Nemadji inició una revisión administrativa, revisó y examinó los procesos para mejorar la seguridad e implementó otros controles diseñados para evitar que vuelva a ocurrir un incidente similar. Además, Nemadji también mejoró la capacitación de nuestro personal para identificar y reaccionar ante correos electrónicos de phishing.

Además de notificar a las personas que podrían estar afectadas por este incidente, hemos notificado a la Oficina Federal de Investigación (FBI). También notificaremos a la Fiscalía General del Estado y a la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de los Estados Unidos, tal como lo exige la ley.

# Qué puede hacer

Para ayudar a disipar las preocupaciones y a recuperar la confianza después de este incidente, hemos contratado los servicios de Kroll para ofrecer un control de identidad sin costo para usted por un año. Kroll es un proveedor mundial líder en reducción y reacción ante riesgos y su equipo tiene una amplia experiencia en ayudar a personas que expusieron de forma involuntaria datos confidenciales. Sus servicios de control de identidad incluyen el control de crédito, la consulta por fraudes y la restauración por robo de identidad.

Visit my.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until September 29, 2019 to activate your identity monitoring services.

Membership Number: << Member ID>>>

To receive credit services by mail instead of online, please call 1-800-491-4740. Additional information describing your services is included with this letter.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

#### For More Information

If you have questions, please call 1-800-491-4740, Monday through Friday from 8:00 a.m. to 5:30 p.m. Pacific Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Heidi Lourey Compliance Officer



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

## **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

## **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

## **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>&</sup>lt;sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Visite my.idMonitoringService.com para activar y aprovechar los servicios de control de identidad.

Tiene hasta 29 de septiembre, 2019 para activar sus servicios de control de identidad.

Número de membresía: << Member ID>>

Llame al 1-800-491-4740 para recibir servicios de crédito por correo, en vez de recibir servicios en línea. En esta carta se incluye información adicional sobre sus servicios.

Revise la sección adjunta "Recursos adicionales" que se incluye en esta carta. Esta sección describe otros pasos que puede tomar para ayudar a protegerse, incluidas recomendaciones de la Comisión Federal de Comercio con respecto a la protección ante robo de identidad y detalles sobre cómo colocar una alerta de fraude o un congelamiento de seguridad en su historial de crédito.

#### Para obtener más información

Si tiene alguna pregunta, llame al 1-800-491-4740, de lunes a viernes, de 8:00 a.m. a 5:30 p.m., hora del Pacífico. Tenga su número de membresía a mano.

Para nosotros es importante proteger su información. Confiamos que los servicios que le ofrecemos demuestran nuestro compromiso constante con su seguridad y satisfacción.

Atentamente.

Heidi Lourey

Responsable de cumplimiento



#### APROVECHE LOS SERVICIOS DE CONTROL DE IDENTIDAD

Se le ha proporcionado acceso a los siguientes servicios¹ de Kroll:

## Control de crédito de oficina única.

Recibirá alertas cuando haya cambios en sus datos de créditos, por ejemplo cuando se solicite una nueva línea de crédito a su nombre. Si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraude de Kroll, quien podrá ayudarlo a determinar si es un indicio de un robo de identidad.

## Consulta por fraude

Tiene acceso ilimitado a consultas con un especialista en fraude de Kroll. El soporte incluye la demostración de las maneras más efectivas de proteger su identidad; la explicación de sus derechos y protecciones en virtud de la ley; la asistencia con las alertas de fraude y la interpretación de cómo se accede y utiliza la información personal, incluida la investigación de actividades sospechosas que puedan estar relacionadas con un evento de robo de identidad.

## Restauración por robo de identidad

Si usted sufre un robo de identidad, un investigador licenciado y experimentado de Kroll trabajará en su nombre para resolver los problemas relacionados. Tendrá acceso a un investigador dedicado, que comprende sus problemas y puede realizar la mayoría del trabajo por usted. Su investigador puede buscar a fondo para descubrir el alcance del robo de identidad y luego trabajar para resolverlo.

<sup>&</sup>lt;sup>1</sup> El sitio web de activación de Kroll es únicamente compatible con la versión actual o una versión anterior de Internet Explorer, Chrome, Firefox y Safari. Para recibir servicios de crédito, debe ser mayor de 18 y tener un crédito establecido en los Estados Unidos, tener un número de seguro social a su nombre y tener un domicilio de residencia en los Estados Unidos asociado a su historial de crédito.

## **ADDITIONAL RESOURCES**

#### **Monitor Accounts**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank account statements, credit or debit card statements, health insurance policy statements, credit reports, and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-
		report-services

In order to request a security freeze, you will need to provide the following information:

- 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- 2. Social Security number;
- 3. Date of birth;
- 4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- 5. Proof of current address, such as a current utility bill or telephone bill;
- 6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
- 7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-	www.equifax.com/personal/credit-
	resource/place-fraud-alert	report-services

#### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

## **RECURSOS ADICIONALES**

## Control de cuentas

Le alentamos a que esté atento a incidentes de robo de identidad y fraude, que revise sus resúmenes de cuentas bancarias, resúmenes de tarjetas de crédito o débito, informes de pólizas de seguros médicos, informes crediticios y formularios de explicación de beneficios para detectar actividades sospechosas. Conforme a la ley de los Estados Unidos, usted tiene derecho a solicitar un informe crediticio anual gratis de cada una de las tres principales agencias de informes de crédito. Para solicitar su informe crediticio gratuito, visite www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. También puede ponerse en contacto directamente con las tres principales agencias de informes de crédito para solicitar una copia gratuita de su informe crediticio.

Tiene el derecho de colocar un "congelamiento de seguridad" sobre su informe crediticio, que evitará que una agencia de informes de solvencia divulgue información en su informe crediticio si no lo autoriza de forma explícita. El congelamiento de seguridad está diseñado para evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Sin embargo, debe saber que usar un congelamiento de seguridad para poder controlar quién obtiene acceso a la información personal y financiera de su informe crediticio puede demorar, interferir o impedir la autorización oportuna de cualquier solicitud o petición que usted haga a posteriori con respecto a un préstamo, crédito o hipoteca nueva o a cualquier otra cuenta que implique la concesión de un crédito. Conforme a la ley federal, no le pueden cobrar por colocar o quitar un congelamiento de seguridad de su informe crediticio. Si desea colocar un congelamiento de seguridad, póngase en contacto con las principales agencias de informes de solvencia que se mencionan a continuación:

Experian	TransUnion	Equifax
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit- report-services

Para poder solicitar un congelamiento de seguridad, deberá proporcionar la siguiente información:

- 1. Nombre completo (incluida la inicial del segundo nombre, así como los sufijos Jr., Sr., II, III, etc.)
- 2. Número de Seguro Social
- 3. Fecha de nacimiento
- 4. Si se mudó en los últimos cinco (5) años, indique los domicilios en los que vivió en el transcurso de este tiempo.
- 5. Comprobante del domicilio actual, como una factura actual de un servicio o una factura telefónica
- 6. Una fotocopia legible de un documento de identidad emitido por un organismo gubernamental (licencia de conducir estatal o documento de identidad, identificación militar, etc.).
- 7. Si usted es víctima de un robo de identidad, incluya una copia de la denuncia policial, del informe de investigación o de la denuncia efectuada ante un organismo de seguridad encargado de tratar con el delito de robo de identidad.

Como alternativa a un congelamiento de seguridad, tiene el derecho a incluir sin cargo en su historial una "alerta de fraude" preliminar o prolongada. Una alerta de fraude preliminar es una alerta de 1 año, que se incluye en el historial de crédito del consumidor. Si una empresa ve una alerta de fraude en el historial de crédito de un consumidor, debe tomar medidas para verificar la identidad del consumidor antes de conceder un crédito nuevo. Si usted fue víctima de un robo de identidad, tiene derecho a implementar una alerta de fraude prolongada, que es una alerta que dura siete años. Si desea colocar una alerta de fraude, póngase en contacto con cualquiera de las agencias que se mencionan a continuación:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-	www.equifax.com/personal/credit-
	resource/place-fraud-alert	report-services

# Información adicional

Además, puede instruirse sobre el robo de identidad, las alertas de fraude, los congelamientos de seguridad y los pasos que puede seguir para protegerse. Para ello, póngase en contacto con las agencias de informes de solvencia, con la Comisión Federal de Comercio o con el fiscal general del Estado.

Puede acercarse a la Comisión Federal de Comercio de las siguientes maneras: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. La Comisión Federal de Comercio también sugiere que toda aquella persona que haya descubierto que su información ha sido utilizada indebidamente presente una denuncia ante ellos. Puede obtener más información sobre cómo presentar una

**For North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

This document includes an important notice. If you cannot read this attached document, please call 1-800-491-4740 for translation help.

## **TAGALOG**

Ang liham na ito ay naglalaman ng mahalagang impormasyon. Kung hindi ninyo nababasa ang kalakip na liham, mangyaring tumawag sa 1-800-491-4740 upang magkaroon ng tulong sa pagsasalin sa Tagalog/Filipino.

# **RUSSIAN**

В этомписьмесодержитсяважнаяинформация. ЕслиВынеможетепрочитатьприлагаемоеписьмо, позвонитепономеру 1-800-491-4740, и Вамбудутпредоставленыуслугипереводанарусскийязык.

# **KOREAN**

이서신에는 중요한정보가 포함되어있습니다. 동봉된서신을 읽으실수 없으면 1-800-491-4740 로전화하여한국어번역지원을 받으십시오.

#### **ARMENIAN**

Այս նամակը պարունակում է կարևոր տեղեկություններ։ Եթե ներփակ նամակըչեք կարող կարդալ, խնդրվում է կապվեք 1-800-491-4740 հեռախոսահամարով, օգնություն ստանալ Հայերեն լեզվով։

# **CHINESE (Cantonese)**

这封信包含了重要信息。如果您无法阅读随附的信件,请致电1-800-491-4740 寻求广东话翻译援助。 這封信包含了重要信息。如果您無法閱讀隨附的信件,請致電1-800-491-4740 尋求廣東話翻譯援助。

## **VIETNAMESE**

Thư này bao hàm thông tin quan trọng. Nếu quý vị không đọc được thư đính kèm, vui lòng gọi 1-800-491-4740 để được giúp đỡ thông dịch trong tiếng Việt.

## **CHINESE** (Mandarin)

这封信包含了重要信息。如果您无法阅读随附的信件,请致电1-800-491-4740 寻求普通话翻译援助。 這封信包含了重要信息。如果您無法閱讀隨附的信件,請致電1-800-491-4740 尋求國語翻譯援助。

#### IRANIAN/PERSIAN

ایننامهحاوی اطلاعاتمهمی میباشد. اگر نامهضمیمهر انمیتو انیدبخو انید, لطفاًبر ای کمکبهز بانفار سی باشمار هتلفن –4740-491-800-1

# **ARABIC**

هذه الرسالة تحتوي على معلومات هامة. إذا لم تتمكن من قراءة الرسالة المرفقة، يرجى الاتصال على 4740-491-800-1 للحصول على معلومات هامة. إذا لم تتمكن من قراءة في الترجمة إلى العربية.

demanda por medio de la información de contacto que se indica a continuación. Tiene derecho a hacer una denuncia policial si fue víctima de un robo de identidad o fraude. Tenga en cuenta que, para poder hacer una denuncia ante una autoridad policial por robo de identidad, probablemente necesite presentar alguna prueba de que fue víctima de ese delito. También se debe denunciar ante agentes policiales ocasiones de robo de identidad presuntas o reales. Este aviso no fue retrasado por las autoridades policiales.

Los residentes de Carolina del Norte, pueden comunicarse con el fiscal general en 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 o al 1-919-716-6400, www.ncdoj.gov.

Este documento incluye un aviso importante. Si no puede leer este documento adjunto, por favor llame 1-800-491-4740 para obtener ayuda de traducción.

#### **TAGALOG**

Ang liham na ito ay naglalaman ng mahalagang impormasyon. Kung hindi ninyo nababasa ang kalakip na liham, mangyaring tumawag sa 1-800-491-4740 upang magkaroon ng tulong sa pagsasalin sa Tagalog/Filipino.

## **RUSSIAN**

В этомписьмесодержитсяважнаяинформация. ЕслиВынеможетепрочитатьприлагаемоеписьмо, позвонитепономеру 1-800-491-4740, и Вамбудутпредоставленыуслугипереводанарусскийязык.

## **KOREAN**

이서신에는 중요한 정보가 포함되어있습니다. 동봉된서신을 읽으실수 없으면 1-800-491-4740 로전화하여한국어 번역 지원을 받으십시오.

#### **ARMENIAN**

Այս նամակը պարունակում է կարևոր տեղեկություններ։ Եթե ներփակ նամակըչեք կարող կարդալ, խնդրվում է կապվեք 1-800-491-4740 հեռախոսահամարով, օգնություն ստանալ Հայերեն լեզվով։

# **CHINESE (Cantonese)**

这封信包含了重要信息。如果您无法阅读随附的信件,请致电1-800-491-4740 寻求广东话翻译援助。 這封信包含了重要信息。如果您無法閱讀隨附的信件,請致電1-800-491-4740 尋求廣東話翻譯援助。

# **VIETNAMESE**

Thư này bao hàm thông tin quan trọng. Nếu quý vị không đọc được thư đính kèm, vui lòng gọi 1-800-491-4740 để được giúp đỡ thông dịch trong tiếng Việt.

# **CHINESE (Mandarin)**

这封信包含了重要信息。如果您无法阅读随附的信件,请致电1-800-491-4740 寻求普通话翻译援助。 這封信包含了重要信息。如果您無法閱讀隨附的信件,請致電1-800-491-4740 尋求國語翻譯援助。

#### IRANIAN/PERSIAN

ایننامهحاوی اطلاعاتمهمی میباشد. اگر نامهضمیمهر انمیتو انیدبخو انید, لطفاًبر ای کمکبهز بانفار سی باشمار هتلفن –4740-491-800-1

# **ARABIC**

هذه الرسالة تحتوي على معلومات هامة. إذا لم تتمكن من قراءة الرسالة المرفقة، يرجى الاتصال على 4740-491-800-1 للحصول على معلومات هامة. إذا لم تتمكن من قراءة في الترجمة إلى العربية.